**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media

**Network security**

1. What types of physical security measures can be put in place?

Security measures to protect your computer include physical measures, such as locks and alarms to warn of intruders, login systems with usernames and passwords, firewalls, malware protection, encryptions, and secure websites

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

A login system that would help to protect a network would include a username specific to the individual user (one that is easy to remember) and a password that is known only by that user. A password should be no shorter than 8 digits, include numbers as well as letters, not be a name that could be easily guessed, and be changed every month.

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters the information coming through an Internet connection into an internal network. Any data that is unwanted is blocked access.

1. What are the main purposes of firewalls and how are these purposes achieved?

Firewalls are designed to block unwanted data from entering the network, which is separated from wanted data by filtering out the IP addresses of computers trying to access the network, blocking access to domain names, banning particular protocols from accessing particular servers, and certain words or phrases. Firewalls can also restrict an employee’s access to sensitive information, for example the payroll database.

1. Why do firewalls use 2 separate NICs?

Firewalls use two separate NICs because one is used to connect to the internal network and the other the outside world. They then filter out any unwanted data that is potentially malicious, all of which passes through the CPU of the server sitting between the two NICs.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware refers to malicious software and includes spyware, adware, Trojan horses, worms and viruses. These all leave your computer at risk, whether to spy on what you are doing, or damage or wipe your computer.

**Encryption**

1. What is encryption?

Encryption is the process of translating data into a secret code that can only be read by authorised viewers.

1. Describe the nature of WPA or WPA2.

Wi-Fi protected access is a security protocol for use by wireless LANs. It provides security by encrypting data over radio waves so that it is protected during transmission.

1. What is encrypted data known as?

It is known as ciphertext.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

These transactions are encrypted by industry standard 128-bit SSL encryption, which provides a secure connection on the internet.

1. What is digital identification certificate technology based on?

Digital identification certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

1. Describe the nature of Secure sockets layer (SSL) protocol.

SSL protocol is a cryptographic protocol that provides a secure connection to the internet. When a web browser tries to access a secure domain name, the SSL protocol authenticates the server (website) and the client (web browser)

**Physical design of networks**

1. What is the role of a network diagram?

A network diagram is a schematic method of showing the physical devices and communications lines in a network. Straight lines represent cables, and icons are used to represent devices.